(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 15/00

(11) 공개번호 특2001-0044823
(43) 공개일자 2001년06월05일

(21) 출원번호 10-2001-0016423
(22) 출원일자 2001년03월29일

(71) 출원인 주식회사 세이프텍 이종우
서울특별시 송파구 송파1동 48-18번지 유니온빌딩
(72) 발명자 이종우
경기 용인시 수지읍 풍덕천리 698-2 한성아파트 101동 901호
(74) 대리인 손창규

심사청구 : 없음

(54) 컴퓨터에서 사용자 인증이 필요한 자료의 보호방법 및그에 관한 시스템

요약

본 발명은 인터넷에 연결되어 있는 컴퓨터에서 사용자의 인증이 필요한 자료의 보호 방법 및 그에 관한 시스템에 관한 것으로서, 상세하게는, 인터넷 환경하에서 필요한 인증서나 유료로 판매되는 소프트웨어 등의 파일에 대한 접근요청을 검출하여 인증된 사용자에 의한 경우에만 실행을 허용하도록 구성되어 있다. 발명의 방법 및 시스템에 따르면, 인터넷 환경하에서의 인증서 등을 완벽하게 보호할 수 있으므로 거래의 신뢰도 및 사용자의 안전성을 확보할 수 있고, 음악 파일과 같이 손쉽게 복제가 가능한 파일을 사용자 본인이나 타인의 해킹에 의해 불법 복제하는 것을 방지할 수 있다.

대표도

도2

명세서

도면의 간단한 설명

도 1은 인터넷 환경하에서 사용자 컴퓨터가 자료 제공 서버에 연결되어 동작하는 것을 설명하는 개략적 구성도이고;

도 2는 본 발명의 인증자료 관리 시스템 및 그와 관련된 컴퓨터 시스템의 일부 구성에 관한 개략적 구성도이고;

도 3a 내지 3c는 인증자료 관리 시스템에 의한 동작 과정의 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 인터넷에 연결되어 있는 컴퓨터에서 사용자의 인증이 필요한 자료의 보호 방법 및 그에 대한 시스템에 관한 것으로서, 상세하게는, 인터넷 환경하에서 필요한 인증서나 유료로 판매되는 소프트웨어 등의 파일에 대한 접근요청을 검색하여 인증된 사용자에 의한 경우에만 실행을 허용하도록 구성되어 있다.

인터넷의 빠른 보급으로 인하여, 은행거래, 증권거래, 홈 쇼핑과 같은 종래의 일반 상거래는 더 이상 오프라인상으로 한정되지 않고 인터넷과 같은 온라인으로 확장되고 있다. 문서 교환 등의 사무업무도 인터넷의 신속성 및 편리성에 기인하여 온라인상에서 진행되고 있다.

그러나, 비접촉, 비대면적 특성을 지닌 인터넷 기반의 상거래 및 전자문서교환 등은 거래 상대방의 신원확인, 거래내용의 위 변조 및 거래사실 부인 방지를 위한 안전장치를 마련할 필요가 있는데, 인터넷상에서 이러한 거래 상대방의 신원 및 신용을 확인하거나 증명할 수 있는 것이 이른바 인증서(Certificate)이다. 따라서, 인증서는 전자 거래 상대방의 신원확인(Authentication), 전송되는 정보의 변질여부확인(Integrity), 전자거래 상대방간 정보 송수신 여부에 대한 부인방지(Non-repudiation) 등의 서비스를 가능하게 한다. 이러한 인증서는 신원확인 등을 거친 후 인증기관으로부터 다운로드받아 사용자(Client)의 컴퓨터 시스템에 저장되게 되고, 사용자가 관련 전자거래를 행할 때 비밀번호 등을 입력하게 함으로써 인증절차를 거치게 된다. 따라서, 인증서는 사이버 세계에서의 인감과 같은 중요한 역할을 담당하므로, 이를 타인이 사용하게 될 경우에는 커다란 피해를 가져오게 된다.

한편, 전자 상거래의 하나의 유형으로서, 다운로드의 형태로 제품을 제공할 수 있는 분야, 즉,

게임 프로그램, 유틸리티 프로그램, MP3 등의 음악파일 등과 같이 소프트웨어의 온라인 판매 분야에서는 불법 복제가 심각한 문제로서 대두되고 있다. 더욱이, 최근에는 인터넷을 통해 무료로 다운로드 받는 MP3 음악파일의 저작권 침해문제가 제기되고 있다. 따라서, 소프트웨어의 불법 복제는 단순히 오프라인상에서의 재산권 침해를 넘어서 오라인상의 문제로 확대되고 있고, 하나의 사회적 문제로서 이슈화되고 있는 실정이다.

소프트웨어의 불법 복제를 막는 방법으로서 현재 사용되고 있는 대표적인 예를 살펴보면, 시리얼 번호 입력법, 불법 복제 방지용 슬롯(slot)을 프린터 포터(port)에 설치하는 방법, 기타 워터마킹(watermaking) 법 등이 있다. 그러나, 시리어 번호 입력법은 근본적인 방지책은 아니므로 직접 확인하지 않고서는 암암리에 행해지는 불법 복제를 막을 수 없으며, 슬롯 설치법은 사용자가 직접 장치에 설치하여야 하므로 불편하고 저가 소프트웨어의 경우에는 가격면에서 보편적으로 채택하기 어려우며, 워터마킹법은 사용자가 사용하는 것을 가능케 하는 1:1 개념으로서 이미 이에 관한 해킹 프로그램이 개발되어 악용되고 있는 실정이다.

발명이 이루고자하는 기술적 과제

이러한 제반 문제점은, 사용자 자신의 자의적 의사이든 타의적 행위(해킹 등)이든 간에, 전자 상거래 등에서의 인증서와 유료배급 소프트웨어 등과 같이 사용자의 컴퓨터 시스템내에 저장되어 있는 중요한 자료의 파일를 함부로 사용하거나 복제할 수 없게 한다면 방지될 수 있다.

따라서, 본 발명은 인터넷을 통한 전자 상거래에 사용되는 인증서와 역시 인터넷을 통해 판매(유료로 배급)되는 소프트웨어의 불법적인 인출을 막기 위하여, 상기 인증서 및 소프트웨어 파일의 불법적인 접근 및 복제 등을 근본적으로 차단할 수 있는 방법 및 시스템의 제공을 목적으로 한다.

발명의 구성 및 작용

이러한 목적을 해결하기 위하여, 본 발명은 인터넷에 연결되어 있는 컴퓨터상의 인증자료 파일을 보호하는 방법으로서,

인터넷을 통해 다운로드받은 특정 인증자료 파일을 컴퓨터 시스템내의 저장장치에 저장하고, 컴퓨터 운영체제의 파일 시스템내에서 동작하는 인증자료 관리 시스템이 상기 인증자료 파일이 저장되어 있는 디렉토리를 보호대상 디렉토리로서 관리정보 파일에 등록하는 제 1 과정;

상기 인증자료 관리 시스템은 컴퓨터 시스템으로부터 접근이 요청된 파일이 상기 관리정보 파일에 등록된 디렉토리상의 인증자료 파일인 경우, 그것이 인증된 사용자에 의한 것인지를 인증절차를 통해 확인하는 제 2 과정;

상기 인증절차 결과, 상기 접근 요청이 인증된 사용자로 판단된 경우에는 실행을 허여하고, 그렇지 않을 경우에는 실행을 허여하지 않는 제 3 과정을 포함하는 것으로 구성되어 있다.

상기 인증자료 파일은 인터넷 환경하에서 사용자 인증이 필요한 자료들의 파일들로서, 전자상거래나 문서교환을 위한 인증서 프로그램, MP3 프로그램 등을 예로 들면, 이들을 구성하는 파일들 중에 프로그램의 실행과 관련된 파일 이외에 등록정보, 회원정보, 특정 데이터 등에 관한 파일로서 사용자에 의해 임의로 변경되는 것이 금지된 모든 파일을 의미한다. 따라서, MP3 프로그램의 경우, 각각의 곡에 관한 파일이나 곡들의 패키지에 관한 파일, 또는 이용/거래 내역서 파일 등이 인증자료 파일이 될 수 있다.

상기 인증자료 관리 시스템은 그것의 관리정보 파일에 등록된 디렉토리상에 저장되어있는 인증자료 파일에 대한 접근 요청이 인증된 사용자에 의해 실행되는 것인지 등을 판단하여 처리하는 상기 과정을 수행할 수 있는 프로그램으로서, 상기 인증자료 파일을 제공하는 "자료 제공자 서버"에 의해 역시 제공될 수 있는데, 인터넷으로 다운로드받아 자동으로 인스톨(install)되거나 또는 오프라인 상으로 부여받아 사용자가 인스톨한다.

상기 인증자료 관리 시스템은 앞서 설명한 바와 같이 컴퓨터 운영체제(Operating System: O/S)의 파일 시스템(File System)상에 위치하여 작동되므로, 저장장치상의 인증자료 파일에 대한 접근요청을 모니터링할 수 있다. 일반적으로, O/S의 파일 시스템은 파일에 이름을 붙이고, 저장이나 검색을 위해 논리적으로 이들을 어디에 위치시켜야 하는지 등을 나타낸 계층적인 구조를 가지고 있다. 파일 시스템은 파일의 이름을 붙이는 규칙을 가지고 있는바, 이러한 규칙에는 파일 이름의 길이제한, 어떤 글자들이 사용될 수 있는지 등이 포함되며, 디렉토리 구조를 통하여 파일까지 가는 경로를 설정하는 형식을 또한 포함한다. 파일 시스템을 대별하여 하위 계층과 상위 계층으로 구별할 수 있는데, 하위 계층은 기계어 등과 같이 컴퓨터의 하드웨어의 작동에 가까운 프로그램에 대한 것이다. 본 발명의 상기 인증자료 관리 시스템은 네트워크 파일 시스템 제어부와 같은 상위계층보다는 하드디스크 등의 물리적 제어 계층에 접근하여 동작한다.

인증자료 관리 시스템의 관리정보 파일은 삭제나 복사는 물론 볼 수 없도록 관리되며, 인증자료 관리 시스템은 모든 파일로의 접근 요청을 모니터링해서 위의 관리정보 파일에 등록된 디렉토리상의 인증자료 파일로의 접근을 제어한다. 상기 등록 디렉토리는 보호대상 파일별로 하나 또는 둘 이상을 설정할 수 있으며, 디렉토리 별로 접근 허용 인증절차(예를 들어, 비밀번호 등)를 별도로 부여할 수도 있다.

상기 인증절차의 방법은 비밀번호 사용 방법, 스마트카드(IC 카드) 사용 방법, 온라인으로 자료 공급/판매자 코드확인 방법 등 인증된 사용자에 의한 실행인지를 확인할 수 있는 방법이라면 어느 것이라도 무방하다.

사용자가 필요에 의해 응용프로그램을 실행함으로써, 컴퓨터 시스템에 의해 상기 인증자료 파일로의 접근 요청이 있는 경우, 인증자료 관리 시스템은 이를 검출(detect)하여 접근을 허여할 수 있는 비밀번호 입력 등의 "인증절차"를 요청하게 되고, 올바른 인증결과가 확인된 경우에만 인증자료 파일의 송

출이 이루어진다. 인증확인 결과가 실패한 경우에는 인증자료 파일로의 접근이 허용되지 않게 되는데, 바람직하게는 인증절차의 연속인증실패 횟수를 특정 횟수("연속인증실패 한계 횟수": 비밀번호 입력 방법의 경우에는 "연속입력오류 한계 횟수") 이하로 정하여, 인증되지 않은 사용자에 의한 접근 시도를 차단하는 과정을 포함시킬 수 있다. 바람직하게는 상기 연속인증실패 한계 횟수를 3회 내지 5회로 할 수 있다.

그러나, 이 경우, 인증된 사용자라 하더라도 본의아니게 실수로 연속인증실패 횟수가 상기 한계 횟수를 초과할 수 있으므로, 이러한 문제점을 해결하기 위하여, 인증된 사용자의 재사용을 위한 회복 조치를 취할 수 있게 한다. 예를 들어, 상기 인증자료 관리 시스템은 제품별로 고유코드를 가지고 있고, 최초 인스톨시 인증된 사용자의 설정에 따라 질의/정답 코드를 생성하며, 인증절차상의 연속인증실패 횟수가 상기 한계 횟수를 초과한 경우에는 상기 고유코드와 질의코드를 보여주고 그에 상응하는 정답(제공자 시스템에서 특수연산한 결과)을 제공자로부터 받아서 이를 사용자의 컴퓨터에서 본 시스템의 정답 입력란에 입력하여 사용자 특수 연산을 통해 연산결과를 얻고, 상기 입력받은 특수 연산결과와 제품내의 동일한 특수연산 기능에 의한 연산결과를 비교하여, 동일한 경우에는 인증된 사용자로 간주하여 연속입력오류 횟수를 리셋(최소값으로)하는 별도의 과정을 포함할 수 있다.

경우에 따라서는, 상기 인증절차로서 비밀번호 입력법을 사용하고, 상기 비밀번호를 키로 사용하여 인증자료의 암호화/복호화를 행하여 처리할 수 있도록 구성할 수도 있다. 컴퓨터 시스템내에서 비밀번호에 의한 자료의 암호화/복호화 처리 방법은 본 발명자의 PCT 국제출원 공개공보 WO 01/10079 A1(공개일: 2001. 2. 8.) 등에 공지되어 있으므로 이에 대한 자세한 설명은 생략하지만, 이들 개시 내용은 본 발명의 내용에 합체된다.

경우에 따라서는, 상기 인증절차에서 특정 자료 파일에 대해 단순이용, 쓰기/복제 등을 선택적으로 허여하고 이들의 횟수(단순이용 횟수, 쓰기/복제 횟수) 등에 제한을 두도록 설정할 수도 있는데, 이는 인증자료 제공자가 정하게 되며 인증자료 관리 시스템의 관리정보 파일에 저장되어 관리된다. 상기 단순이용 횟수의 제한이란, 인증자료 제공자가 미리 정한 횟수만큼 인증절차 없이 사용이 가능하도록 하고 횟수가 다하면 상기 관리 시스템이 자동삭제하거나 사용불가하게 하는 것이고, 상기 쓰기/복제 횟수의 제한이란 인증자료 제공자의 설정에 따라 데이터의 변경, 복사 등의 허용횟수를 제한하는 것을 의미한다.

인증자료 파일이 저장되는 디렉토리는 인증자료 제공자에 의해 정해지거나 또는 사용자가 정할 수 있게 할 수도 있다.

본 발명은 또한 상기 방법을 실행할 수 있는 인증자료 관리 컴퓨터 시스템에 관한 것이다. 즉, 인터넷에 연결되어 작동되는 인증자료 관리 컴퓨터 시스템은,

인터넷에 접속하기 위한 통신장치;

인증자료 파일의 제공/판매자의 코드 확인 모듈;

관리정보 파일에 등록된 디렉토리상에 저장된 인증자료 파일로의 접근 요청을 모니터링하여 설정 방식에 따라 사용자의 인증여부를 확인하고 확인결과에 따라 접근 요청을 허여 내지 불허하는, 운영체제의 파일 시스템에 위치하는 인증자료 관리 시스템; 및

인증자료가 저장되는 저장장치를 포함하는 것으로 구성되어 있다.

상기 인증자료 관리 시스템의 관리정보 파일에는 설정 방식으로서 인증자료 파일의 정의, 인증절차의 정의, 제어방법의 정의 등이 포함되어 있다. 상기 인증자료 파일의 정의에는 인증자료가 저장되는 등록 디렉토리 정보 등이 포함되어 있고, 상기 인증절차의 정의에는 비밀번호 입력 방법인지, 자료 제공/판매자 코드 확인 방법인지, IC 카드 사용 방법인지에 대한 정보가 포함되어 있으며, 상기 제어방법의 정의에는 단순이용, 인증절차 이용 등과, 단순이용 횟수, 복사 횟수 등의 정보가 포함되어 있다.

이하 본 발명의 실시예에 따른 도면을 참조하여 발명의 내용을 상술하지만 하기 내용에 의해 본 발명의 범주가 한정되는 것은 아니다.

도 1은 인터넷(300) 환경하에서 사용자 컴퓨터(100)가 인증자료 제공 서버(200)에 연결되어 동작하는 구성이 개략적으로 도시되어 있다. 사용자 컴퓨터(100)에는 앞서 설명한 인증자료 관리 시스템이 위치하는 운영체제상의 파일 시스템(110)과, 자료가 저장되어 있고 그것에 대한 접근 요청이 상기 인증자료 관리 시스템에 의해 제어되는 저장장치(120)가 포함되어 있다. 자료제공 서버(200)는 인증자료 관리 시스템의 프로그램을 제공하고 경우에 따라서는 인터넷(300)을 통해 인증자료를 제공할 수 있는 인터넷 서버로서, 상기 프로그램, 인증자료 파일, 사용자 코드 등에 대한 정보를 저장하고 있는 저장장치(220)와, 사용자 컴퓨터와의 통신, 상기 프로그램 등의 제공 등을 제어하는 관리 엔진(210)을 포함하고 있다.

도 2는 본 발명의 인증자료 관리 시스템 및 그와 관련된 컴퓨터 시스템의 일부 구성이 개략적으로 도시되어 있다.

인증자료 관리 시스템(400)은 시스템 운영체제(O/S: 500)상의 파일 시스템(도 2에는 도시하지 않음: 도 1의 110)에 위치하면서 저장장치(120)에 저장되어 있는 파일들의 접근 요청을 제어하게 된다. 상기 O/S에는 모니터(600) 등과 같은 출력장치와, 마우스(610), 키보드(620), IC 카드 리더기(630) 등과 같은 입력장치가 연동되어 있다. 당해 컴퓨터 시스템은 통신장치(700)에 의해 인터넷(300)에 연결되어 통신이 이루어지고, 파일의 제공/판매자의 코드 확인 모듈(800)이 통신장치(700)에 연결되어 있어서 인증자료 관리 시스템(400)을 특정하게 된다. 인증자료 관리 시스템(400)에는 관리정보 파일(410)이 포함되어 있는데, 여기에는 인증자료 파일의 정의(등록 디렉토리 정보 등), 인증방법의 정의(비밀번호 입력 방법, 자료 제공/판매자 코드 확인방법, IC 카드 사용방법 등), 제어방법의 정의(단순이용, 인증절차 이용 등과 단순이용 횟수, 복사 횟수 등) 등이 포함되어 있다.

도 2에는 더욱 자세한 기타의 구성요소들이 도시되어 있지 않지만, 본 발명이 속한 분야에서 통

상의 지식을 가진 자("당업자")라면, 본 발명의 실시에 필요한 구성요소들을 본 명세서의 내용을 바탕으로 충분히 인식할 수 있을 것이다.

도 3a 내지 3c는 인증자료 관리 시스템에 의한 동작 과정의 흐름도가 개시되어 있다. 도 3a를 참조하면, 컴퓨터를 부팅(booting)하여 O/S가 구동되게 되면, 인증자료 관리 시스템의 동작이 시작되게 된다. 컴퓨터가 구동되는 동안에는 인증자료 관리 시스템은 항상 동작중에 있게 된다. 인용자료 제공자에 의해 설정된 디렉토리 정보파일 및 비밀번호의 한계횟수 정보파일이 로딩(loading)되어 버퍼에 저장된다(S100). 또한, 인용자료 파일의 단순이용 횟수, 복제 횟수 관리정보 파일이 로딩되어 버퍼에 저장된다(S110). 모든 파일에 대한 접근을 모니터링하여, 관리정보 파일에 등록된 디렉토리에 저장되어 있는 인증자료 파일에 대한 접근 요청을 검출한다(S120). 접근 요청이 인증절차(비밀번호)를 사용하는 파일에 대한 접근 요청인지 아니면 단순이용 파일 등에 대한 접근 요청인지를 판단한다(S130).

접근 요청이 인증절차(비밀번호)를 사용하는 파일에 대한 접근 요청인 경우(Yes)의 과정이 도 3b에 도시되어 있는데, 이 경우에는 연속인증실패 횟수(비밀번호 연속입력오류 횟수)가 연속인증실패 한계횟수를 초과한 상태인지 여부를 판단한다(S200). 예를 들어, 비밀번호 입력 횟수가 연속입력오류 한계횟수를 넘지 않은 경우(No)에는, 비밀번호 입력창을 컴퓨터 모니터에 표시하고 비밀번호를 입력받는다(인증절차 요구: S210). 해당 디렉토리 정보관리 파일의 비밀번호와 입력받은 비밀번호를 비교하여(인증확인: S211), 비밀번호가 상호 동일한지 여부(인증성공 여부)를 판단한다(S212). 두 비밀번호가 동일한 경우(인증성공: Yes)에는 해당 연속인증실패 횟수(비밀번호의 연속입력 오류 횟수)를 리셋(reset)하고(S220), 해당 파일에 대한 접근을 허용한다(S221). 이 경우라도 해당 파일에 대한 복사 및 쓰기의 접근은 통제한다. 만일, 두 비밀번호가 동일하지 않은 경우(인증실패: No)에는 연속인증실패 횟수(비밀번호의 연속입력오류 횟수)를 증가시키고(S230), 해당 파일에 대한 접근을 금지시킨다(S231).

상기 S200에서 비밀번호 입력 횟수가 연속입력오류 한계 횟수를 넘은 경우(Yes)에는 제품의 고유코드를 화면에 보여주고 질의코드를 생성하여 이를 사용자의 화면에 보여주어, 사용자에게 해당 질의코드에 대한 정답을 입력하도록 요구하고 정답을 입력받는다(S240). 그러면, 다음 단계로 내부에서 계산한 정답과 입력받은 정답을 비교한다(S241). 비교 결과(S242) 상호 동일한 경우(Yes)에는 해당 연속인증실패 횟수(비밀번호의 연속입력오류 횟수)를 리셋하고(S243), 해당 파일에 대한 접근을 허여한다(S221). 반면에 상호 동일하지 않은 경우(No)에는 해당 파일에 대한 접근을 금지시킨다(S231).

상기 S130에서 접근 요청이 단순이용 파일, 쓰기/복사 파일에 대한 접근 요청인 경우(No)의 과정이 도 3c에 도시되어 있는데, 이 경우에는 쓰기/복사 등에 관한 것인지 또는 단순 이용에 관한 것인지를 판단한다(S300).

판단 결과, 단순이용인 경우에는 이용 정보를 읽고(S310), 이용 횟수가 무제한인지를 판단한다(S311). 무제한인 경우(Yes)에는 이용 접근을 허용하고(S320), 무제한이 아닌 경우(No)에는 횟수 제한을 초과하였는지를 판단한다(S330). 판단 결과, 횟수 제한을 초과하지 않은 경우(No)에는 이용 접근 횟수를 증가(+1)시켜 기록하고(S340), 이용 접근을 허용한다(S341). 횟수 제한을 초과한 경우(Yes)에는 이용 횟수가 초과되었음을 사용자의 컴퓨터 모니터에 표시하고(S350)하고, 접근을 중단시킨다(S351).

상기 S300에서의 판단 결과, 쓰기/복사 등에 관한 것인 경우에는 해당 파일에 대한 접근 요청 횟수를 읽어 제한 횟수와 비교한다(S360). 이 때, 제한 횟수가 무제한인 경우에는 무조건 허용한다. 한편, 허용 횟수를 비교(S361)한 결과, 허용 횟수를 초과하지 않은 경우(No)에는 해당 사용 횟수를 증가(+1)시켜 기록하고(S370), 접근을 허용하게 된다(S371). 비교 결과, 허용 횟수를 초과한 경우(Yes)에는 이용 횟수가 초과되었음을 사용자의 컴퓨터 모니터에 표시하고(S350)하고, 접근을 중단시킨다(S351).

본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 상기 내용을 바탕으로 본 발명의 범주내에서 다양한 응용 및 변형이 가능할 것이다. 또한, 상기 개시내용에 자세히 언급되지 않은 것이라도 상기 당업자라면 본 발명의 실시에 필요한 제반 구성 등을 이해할 수 있을 것이다.

발명의 효과

본 발명의 방법 및 시스템에 따르면, 인터넷 환경하에서의 인증서 등을 완벽하게 보호할 수 있으므로 거래의 신뢰도 및 사용자의 안전성을 확보할 수 있고, 음악 파일과 같이 손쉽게 복제가 가능한 파일을 사용자 본인이나 타인의 해킹에 의해 불법 복제하는 것을 방지할 수 있다.

(57) 청구의 범위

청구항 1

인터넷에 연결되어 있는 컴퓨터상의 인증자료 파일을 보호하는 방법으로서,

인터넷을 통해 다운로드받은 특정 인증자료 파일을 컴퓨터 시스템내의 저장장치에 저장하고, 컴퓨터 운영체제의 파일 시스템내에서 동작하는 인증자료 관리 시스템이 상기 인증자료 파일이 저장되어 있는 디렉토리를 보호대상 디렉토리로서 관리정보 파일에 등록하는 제 1 과정;

상기 인증자료 관리 시스템은 컴퓨터 시스템으로부터 접근이 요청된 파일이 상기 관리정보 파일에 등록된 디렉토리상의 인증자료 파일인 경우, 그것이 인증된 사용자의 실행에 의한 것인지를 인증절차를 통해 확인하는 제 2 과정;

상기 인증절차 결과, 상기 접근 요청이 인증된 사용자의 실행으로 판단된 경우에는 실행을 허여하고, 그렇지 않을 경우에는 실행을 허여하지 않는 제 3 과정을 포함하는 것으로 구성되는 것을 특징으로 하는 컴퓨터 상에서 사용자 인증이 필요한 자료의 보호 방법.

청구항 2

제 1항에 있어서, 상기 인증자료 파일은 인터넷 환경하에서 사용자 인증이 필요한 인증서 프로그램, 유료 소프트웨어 프로그램 등의 파일인 것을 특징으로 하는 보호 방법.

청구항 3

제 1항에 있어서, 제 2 과정의 상기 인증절차의 방법은 비밀번호 입력 방법, 스마트카드(IC 카드) 사용 방법, 또는 온라인으로 자료공급/판매자 코드확인 방법이고, 인증절차의 연속인증실패 횟수를 특정 횟수("연속인증실패 한계 횟수") 이하로 정하여 인증되지 않은 사용자의 접근 시도를 차단하는 과정을 포함하는 것을 특징으로 하는 보호방법.

청구항 4

제 3항에 있어서, 상기 인증절차를 비밀번호 입력 방법에 의하고, 상기 비밀번호를 키로 사용하여 인증자료의 암호화/복호화를 행하여 처리하는 것을 특징으로 하는 보호방법.

청구항 5

제 1항 내지 제 4항 중 어느 하나에 있어서, 상기 인증절차에서 특정 자료 파일에 대해 단순이용, 쓰기/복제 등을 선택적으로 허여하고 이들의 횟수(단순이용 횟수, 쓰기/복제 횟수) 등에 제한을 두도록 설정하며, 이러한 설정내용을 인증자료 제공자가 정하고, 그 내용이 상기 인증자료 관리 시스템의 관리정보 파일에 저장되어 관리되는 것을 특징으로 하는 보호방법.

청구항 6

인터넷에 연결되어 있는 컴퓨터에서 사용자 인증을 필요로 하는 자료 파일("인증자료 파일")을 보호하는 시스템으로서,

인터넷에 접속하기 위한 통신장치;

인증자료 파일의 제공/판매자의 코드 확인 모듈;

관리정보 파일에 등록된 디렉토리상에 저장된 인증자료 파일로의 접근 요청을 모니터링하여 설정 방식에 따라 사용자의 인증여부를 확인하고 확인결과에 따라 접근 요청을 허여 내지 불허하는, 운영체제의 파일 시스템에 위치하는 인증자료 관리 시스템; 및

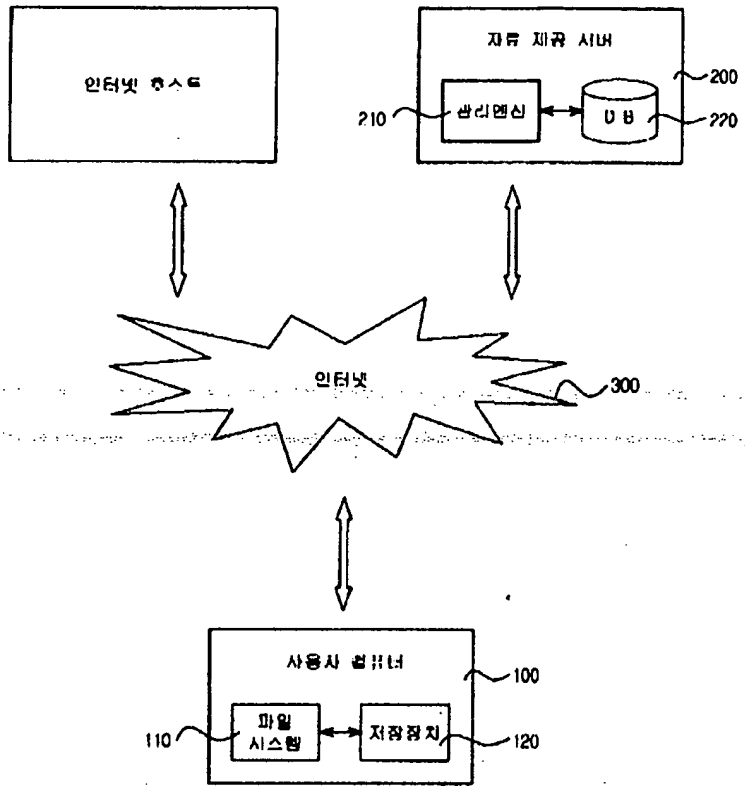
자료가 저장되는 저장장치를 포함하는 것으로 구성되어 있는 것을 특징으로 하는 인증자료 관리 컴퓨터 시스템.

청구항 7

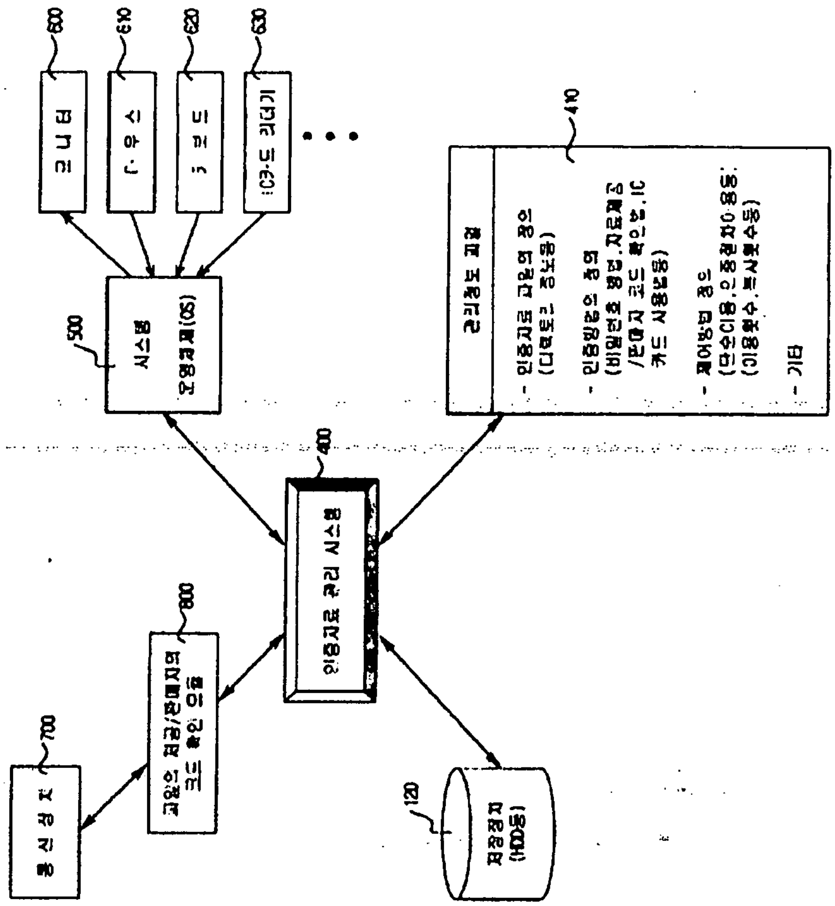
제 6항에 있어서, 상기 인증자료 관리 시스템의 관리정보 파일에는 설정 방식으로서 인증자료 파일의 정의, 인증절차의 정의, 제어방법의 정의 등이 포함되어 있는 것을 특징으로 하는 인증자료 관리 컴퓨터 시스템.

도면

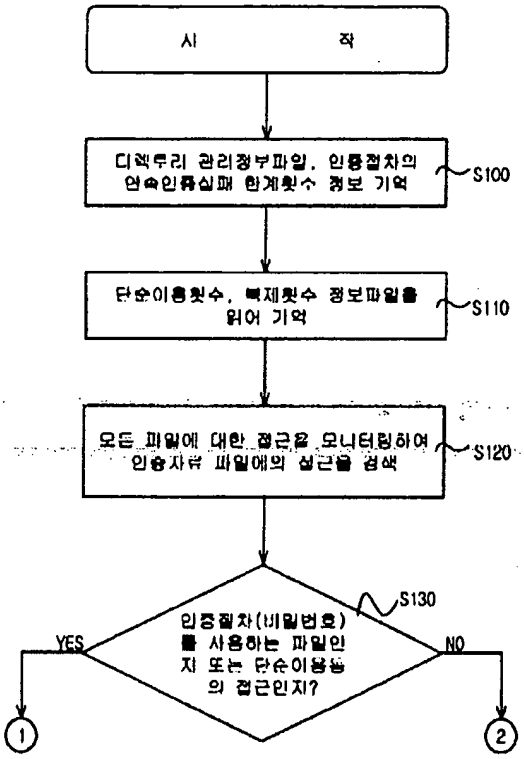
도면1


인터넷 호스트
자료 제공 서버
200
210
관리엔진
DB
220
인터넷
300
사용자 컴퓨터
100
110
파일
시스템
저장장치
120

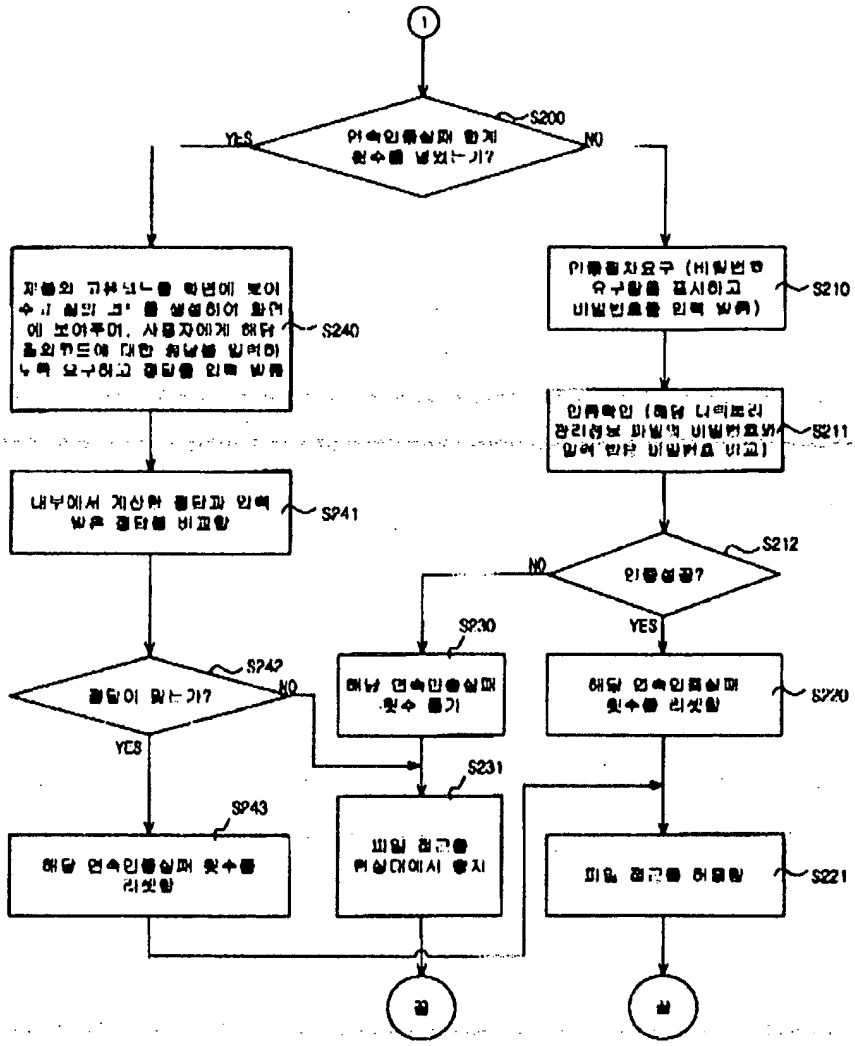
도면2


시스템
운영체제(OS)
500
600
610
620
630
400
410
관리정보 파일
- 기타
800
700
통신장치
120
저장장치
(HDD등)

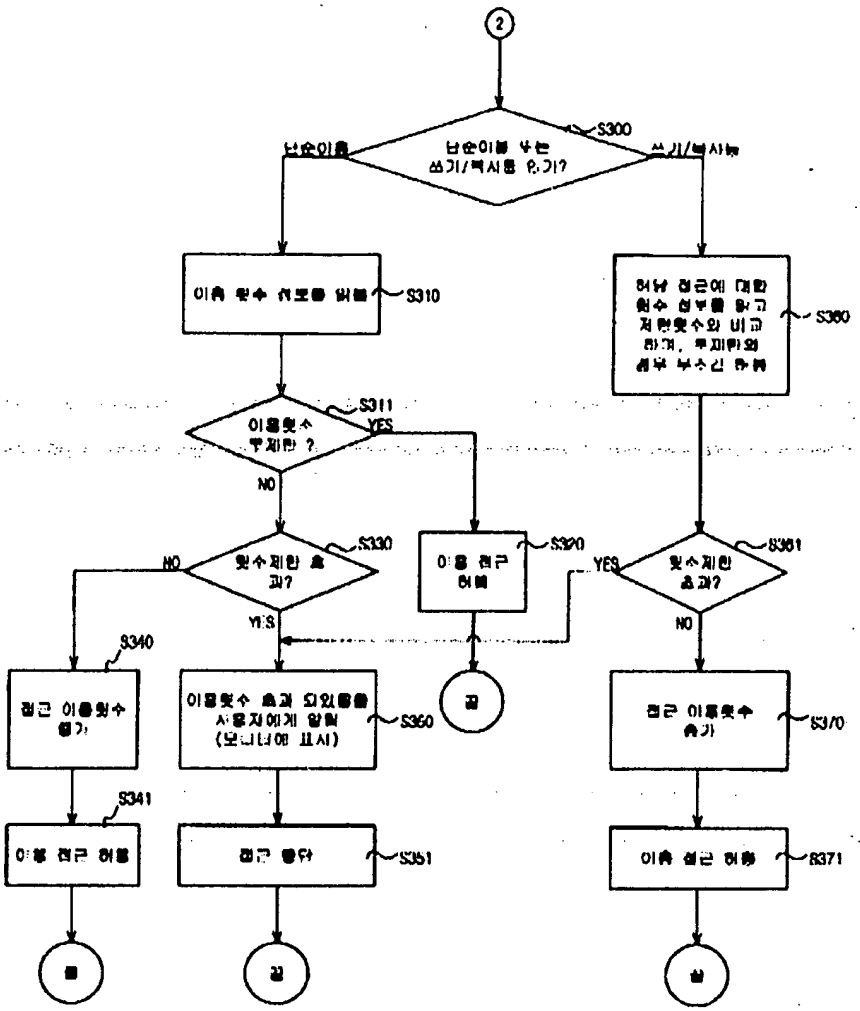
도면3a


시 작
디렉토리 관리정보파일, 인증절차의 연속인증실패 한계횟수 정보 기억
S100
단순이용횟수, 복제횟수 정보파일을 읽어 기억
S110
모든 파일에 대한 접근을 모니터링하여 인증자료 파일에의 접근을 검색
S120
S130
인증절차(비밀번호)를 사용하는 파일인지 또는 단순이용등의 접근인지?
YES
NO
1
2

도면3b


①
S200
YES
NO
S240
S210
S211
S212
NO
YES
S241
S242
NO
YES
S230
S220
S231
S243
S221
②
③

도면3c


2
S300
단순이용
쓰기/복사
S310
S311
YES
NO
S330
NO
YES
S320
S340
S341
S350
S351
S360
S361
S370
S371